LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
CABINET FOR HEALTH SERVICES

In Reference to the Statewide Single Audit
of the Commonwealth of Kentucky

For the Year Ended June 30, 2004

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE (502) 573-0050
FACSIMILE (502) 573-0067

TABLE OF CONTENTS **PAGE**

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Ernie Fletcher, Governor
James W. Holsinger, Jr., MD, Secretary
Cabinet for Health and Family Services

MANAGEMENT LETTER

KRS 43.090(1) requires the Auditor of Public Accounts, upon completion of each audit and investigation, to prepare a report of her findings and recommendations, and to furnish copies of the report to the head of the agency to which the report pertains, and to the Governor, among others. We are providing this letter as our report to the Secretary of the Cabinet for Health and Family Services (CHFS) in compliance with KRS 43.090.

This letter presents the results of the work performed at the Cabinet for Health Services (CHS), as part of our annual audit of the Commonwealth of Kentucky's financial statements. Executive Order 2003-064 has reorganized CHS into CHFS as of December 23, 2004.

In planning and performing our audit of the basic financial statements of the Commonwealth for the year ended June 30, 2004, we considered CHS' internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. However, we noted certain matters involving the internal control and its operation that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the CHS ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and would not necessarily disclose all matters that might be reportable conditions. In addition, because of inherent limitations in internal control, errors or fraud may occur and not be detected by such controls.

As part of our audit of the Commonwealth's basic financial statements, we also performed tests of CHS' compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. The results of those tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards.*

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.AUDITOR.KY.GOV

To the People of Kentucky
Honorable Ernie Fletcher, Governor
James W. Holsinger, Jr., MD, Secretary
Cabinet for Health and Family Services
(Continued)

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with Government Auditing Standards.

Included in this letter are the following:

- Acronym List
- Findings and Recommendations (Reportable Conditions, and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains CHS' findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.auditor.ky.gov.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

Crit Luallen
Auditor of Public Accounts

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Ernie Fletcher, Governor
James W. Holsinger, Jr., MD, Secretary
Cabinet for Health and Family Services

MANAGEMENT LETTER

KRS 43.090(1) requires the Auditor of Public Accounts, upon completion of each audit and investigation, to prepare a report of her findings and recommendations, and to furnish copies of the report to the head of the agency to which the report pertains, and to the Governor, among others. We are providing this letter as our report to the Secretary of the Cabinet for Health and Family Services (CHFS) in compliance with KRS 43.090.

This letter presents the results of the work performed at CHS, as part of our annual Statewide Single Audit of the Commonwealth of Kentucky.

In planning and performing our audit over compliance with requirements applicable to major federal programs, for the year ended June 30, 2004, we considered CHS' internal control in order to determine our auditing procedures for the purpose of expressing an opinion on compliance with requirements applicable to each major federal program and to report on internal control over compliance in accordance with Office of Management and Budget (OMB) Circular A-133 and on the Schedule of Expenditure of Federal Awards (SEFA).

Our consideration of internal control was for the limited purpose described in the preceding paragraph and would not necessarily disclose all matters that might be reportable conditions. In addition, because of inherent limitations in internal control, errors or fraud may occur and not be detected by such controls.

We noted certain instances of noncompliance with requirements applicable to major federal programs. These instances of noncompliance were not considered reportable under standards established by OMB Circular A-133.

As part of our audit of the Commonwealth's basic financial statements, we also performed tests of CHS' compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. The results of those tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards.*

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.AUDITOR.KY.GOV

To the People of Kentucky
Honorable Ernie Fletcher, Governor
James W. Holsinger, Jr., MD, Secretary
Cabinet for Health and Family Services
(Continued)

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with A*uditing Standards Generally Accepted in the United States of America and Government Auditing Standards*.

Included in this letter are the following:

- Acronym List
- Schedule of Expenditures of Federal Awards
- Notes to the Schedule of Expenditures of Federal Awards
- Findings and Recommendations (Federal Noncompliance, and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains CHS' findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.auditor.ky.gov.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

Crit Luallen
Auditor of Public Accounts

LIST OF ABBREVIATIONS/ACRONYMS

AD	Active Directory
APA	Auditor of Public Accounts
BDC	Backup Domain Controllers
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulations
CHFS	Cabinet for Health and Family Services
CHR	Cabinet for Human Resources (former name of the Cabinet for Health Services and the Cabinet for Families and Children)
CHS	Cabinet for Health Services
CMS	Centers for Medicare and Medicaid Services
COT	Commonwealth Office of Technology
DCCM	Direct Cable Connect Manager
DMS	Department of Medicaid Services
DPH	Department for Public Health
FHSC	First Health Services Corporation
FTP	File Transfer Protocol
FY	Fiscal Year
GPO	Group Policy Objects
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
KRS	Kentucky Revised Statutes
LAN	Local Area Network
LSA	Local Security Authority
MMIS	Medicaid Management Information System
NA	Not Applicable
NDC	National Drug Code
OBRA	Omnibus Budget Reconciliation Act
OMB	Office of Management and Budget
PDC	Primary Domain Controller
R&D	Research and Development
SEFA	Schedule of Expenditures of Federal Awards
SMI	Supplementary Medical Insurance
SNMP	Simple Network Management Protocol
SSA	Social Security Administration
SSWAK	Single Statewide Audit of Kentucky
VNC	Virtual Network Computer
WIC	Women, Infants and Children Program

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2004

CFDA #	Program Title	Expenditures Cash	Expenditures Noncash	Provided to Subrecipient
	U.S. Department of Agriculture			
	Direct Programs:			
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children (Note 2)	88,002,978		15,927,294
	Passed Through From Cabinet for Families and Children:			
	Food Stamp Cluster:			
10.561	State Administrative Matching Grants for Food Stamp Program	113,846		
	U.S. Department of Labor			
	Direct Programs:			
17.235	Senior Community Service Employment Program	1,641,946		1,594,277
	U.S. Environmental Protection Agency			
	Direct Programs:			
66.032	State Indoor Radon Grants	481,438		330,923
66.707	TSCA Title IV State Lead Grants-Certification of Lead-Based Paint Professionals	245,806		
	U.S. Department of Energy			
	Passed Through from Cabinet for Families and Children:			
81.042	Weatherization Assistance for Low-Income Persons	7,632		
	Passed Through From Natural Resources And Environmental Protection Cabinet:			
81.502	Paducah Gaseous Diffusion Plant Environmental Monitoring and Oversight	343,693		165,535
	U.S. Department of Education			
	Direct Programs:			
84.186	Safe and Drug-Free Schools and Communities - State Grants	1,616,261		1,616,261

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2004

CFDA #	Program Title	Expenditures Cash	Expenditures Noncash	Provided to Subrecipient
U.S. Department of Health and Human Services				
Direct Programs:				
93.003	Public Health and Social Services Emergency Fund	2,890,626		2,552,187
93.041	Special Programs for the Aging - Title VII, Chapter 3 - Programs for Prevention of Elder Abuse, Neglect, and Exploitation	70,771		70,771
93.042	Special Programs for the Aging - Title VII, Chapter 2 - Long-term Care Ombudsman Services for Older Individuals	187,648		105,137
93.043	Special Programs for the Aging - Title III, Part D - Disease Prevention and Health Promotion Services	338,908		338,908
Aging Cluster:				
93.044	Special Programs for the Aging - Title III, Part B - Grants for Supportive Services and Senior Centers	5,369,421		4,948,055
93.045	Special Programs for the Aging - Title III, Part C - Nutrition Services	7,835,081		7,520,006
93.046	Special Programs for the Aging - Title III, Part D - In-Home Services for Frail Older Individuals	602		(681)
93.048	Special Programs for the Aging - Title IV and Title II - Discretionary Projects	(75)		(75)
93.051	Alzheimer's Disease Demonstration Grants to States	107,204		104,610
93.052	National Family Caregiver Support	1,953,942		1,865,215
93.053	Nutrition Services Incentive Program	1,822,646		1,822,646
93.104	Comprehensive Community Mental Health Services for Children with Serious Emotional Disturbances (SED)	947,881		936,305
93.110	Maternal and Child Health Federal Consolidated Programs	116,135		69,870
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs (Note 3)	944,984	68,050	734,700
93.130	Primary Care Services - Resource Coordination and Development	158,339		89,979
93.136	Injury Prevention and Control Research and State and Community Based Programs	1,097,862		1,084,169

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2004

CFDA #	Program Title	Expenditures Cash	Expenditures Noncash	Provided to Subrecipient
U.S. Department of Health and Human Services (Continued)				
Direct Programs (Continued):				
93.150	Projects for Assistance In Transition from Homelessness (PATH)	300,000		300,000
93.197	Childhood Lead Poisoning Prevention Projects - State and Local Childhood Lead Poisoning Prevention and Surveillance of Blood Lead Levels in Children	683,530		497,600
93.217	Family Planning - Services	6,259,625		5,812,423
93.230	Consolidated Knowledge Development and Application (KD&A) Program	90,527		90,412
93.234	Traumatic Brain Injury - State Demonstration Grant Program	169,500		169,400
93.235	Abstinence Education	1,100,585		1,040,616
93.238	Cooperative Agreements for State Treatment Outcomes and Performance Pilot Studies Enhancement	290,185		188,358
93.243	Substance Abuse and Mental Health Services - Projects of Regional and National Significance	131,881		131,499
93.268	Immunization Grants (Note 3)	2,607,372	14,471,378	1,475,316
93.283	Centers for Disease Control and Prevention - Investigations and Technical Assistance (Note 3)	14,530,567	1,100,802	10,061,885
93.630	Developmental Disabilities Basic Support and Advocacy Grants	1,155,548		731,743
93.767	State Children's Insurance Program (Note 2)	72,325,392		125,786
Medicaid Cluster:				
93.777	State Survey and Certification of Health Care Providers and Suppliers (Note 2)	5,593,098		
93.778	Medical Assistance Program (Note 2)	3,046,629,472		3,061,140
93.779	Centers for Medicare and Medicaid Services (CMS) Research, Demonstrations, and Evaluations	905,088		784,784
93.917	HIV Care Formula Grants	6,938,917		6,888,398
93.931	Demonstration Grants to States for Community Scholarships (Note 4)			
93.940	HIV Prevention Activities - Health Department Based (Note 3)	1,850,064	7,406	1,513,504

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2004

CFDA #	Program Title	Expenditures Cash	Expenditures Noncash	Provided to Subrecipient
U.S. Department of Health and Human Services (Continued)				
Direct Programs (Continued):				
93.944	Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Virus Syndrome (AIDS) Surveillance	136,265		34,476
93.945	Assistance Programs for Chronic Disease Prevention and Control	600,432		412,696
93.958	Block Grants for Community Mental Health Services	5,716,331		5,705,193
93.959	Block Grants for Prevention and Treatment of Substance Abuse (Note 2)	21,420,937		21,415,754
93.977	Preventive Health Services - Sexually Transmitted Diseases Control Grants (Note 3)	880,266	234,972	163,811
93.988	Cooperative Agreements For State-Based Diabetes Control Programs and Evaluation of Surveillance Systems	664,328		577,230
93.991	Preventive Health and Health Services Block Grant	1,794,377		1,639,656
93.994	Maternal and Child Health Services Block Grant to the States	7,466,380		7,242,302
Passed Through From Cabinet for Families and Children:				
93.556	Promoting Safe and Stable Families	873		
93.558	Temporary Assistance for Needy Families	101,317		
93.563	Child Support Enforcement	4,245		
93.568	Low-Income Home Energy Assistance	15,771		
93.569	Community Services Block Grant	16,435		
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund	1,927,537		
93.658	Foster Care - Title IV - E	91,844		
93.667	Social Services Block Grant	15,376		
93.671	Family Violence Prevention and Services/Grants for Battered Women's Shelters - Grants to States and Indian Tribes	123		
93.674	Chafee Foster Care Independent Living	1,037		

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2004

CFDA #	Program Title	Expenditures Cash	Expenditures Noncash	Provided to Subrecipient
Passed Through From Department of Education:				
93.938	Cooperative Agreements to Support Comprehensive School Health Programs to Prevent the Spread of HIV and Other Important Health Problems	109,812		28,000
U.S. Corporation for National and Community Service				
Direct Program:				
Foster Grandparents/Senior Companion Cluster:				
94.011	Foster Grandparent Program	597,829		124,796
NA	Chemical Laboratory Improvement Act	158,941		
Passed Through From Cabinet for Families and Children:				
94.006	AmeriCorps	1,013		
Passed Through From Department of Military Affairs:				
97.040	Chemical Stockpile Emergency Preparedness Program	374,726		115,805
TOTAL CABINET FOR HEALTH SERVICES		3,319,953,121	15,882,608	112,208,675

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS FOR THE YEAR ENDED JUNE 30, 2004

Note 1 - Purpose of the Schedule and Significant Accounting Policies

Basis of Presentation - OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations,* requires a SEFA showing each federal financial assistance program as identified in the *Catalog of Federal Domestic Assistance.* The accompanying schedule includes all federal grant activity for CHS, except those programs administered by state universities, and is presented primarily on the basis of cash disbursements as modified by the application of KRS 45.229. Consequently, certain expenditures are recorded in the accounts only when cash is disbursed. The Commonwealth elected to exclude state universities from the statewide single audit, except as part of the audit of the basic financial statements.

KRS 45.229 provides that the Finance and Administration Cabinet may, "for a period of thirty (30) days after the close of any fiscal year, draw warrants against the available balances of appropriations made for that fiscal year, for the payment of expenditures incurred during that year or in fulfillment of contracts properly made during the year, but for no other purpose." However, there is an exception to the application of KRS 45.229 in that regular payroll expenses incurred during the last pay period of the fiscal year are charged to the next year.

The basic financial statements of the Commonwealth are presented on the modified accrual basis of accounting for the governmental fund financial statements and the accrual basis of accounting for the government-wide, proprietary fund, and fiduciary fund financial statements. Therefore, the schedule may not be directly traceable to the basic financial statements in all cases.

The noncash expenditures presented on this schedule represent the noncash assistance expended by CHS during the period July 1, 2003 through June 30, 2004 using the method or basis of valuation as described in the notes to the SEFA for each program. These noncash assistance programs are not reported in CHS' general-purpose financial statements for the year ended June 30, 2004.

Inter-agency Activity - Certain transactions relating to federal financial assistance may appear in the records of more than one state agency. To avoid the overstatement of federal expenditures, the following policies were adopted for the presentation of the Commonwealth's SEFA:

a) Federal moneys may be received by one state agency and passed through to another state agency where the moneys are expended. Except for pass-throughs to state universities as discussed below, this inter-agency transfer activity is reported by the agency expending the moneys.

   State agencies that pass federal funds to state universities report those amounts as expenditures.

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS FOR THE YEAR ENDED JUNE 30, 2004 (Continued)

Note 1 - Purpose of the Schedule and Significant Accounting Policies (Continued)

Inter-Agency Activity (Continued)

b) Federal moneys received by a state agency and used to purchase goods or services from another state agency are reported in the schedule as an expenditure by the purchasing agency only.

Note 2 - Type A Program

Under the provisions of OMB Circular A-133, a Type A program for the Commonwealth means any program for which total expenditures of federal awards exceeds $20 million for FY 04. All other programs are Type B programs.

Clusters are groups of closely related programs sharing common compliance requirements. A cluster of programs shall be considered as one program for determining Type A programs.

CHS had four cash programs that met the Type A program definition for the year ended June 30, 2004. CHS identified one cluster that included more than one federal program among the Type A programs. These Type A programs were:

CFDA #	Program Title	Expenditures
10.557	Special Supplemental Nutritional Program for Women, Infants, and Children	$ 80,187,442
Medicaid Cluster		
93.777	State Survey and Certification of Health Care Providers and Suppliers	5,782,711
93.778	Medical Assistance Program	2,735,768,588
93.959	Block Grants for Prevention and Treatment of Substance Abuse	21,918,102
93.767	State Children's Insurance Program	69,880,862
	Total Type A Programs	$2,913,537,705

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS FOR THE YEAR ENDED JUNE 30, 2004
(Continued)

Note 3 - Noncash Expenditure Programs

CHS had five (5) noncash programs for the year ended June 30, 2004. These noncash programs and a description of the method/basis of valuation follow:

CFDA #	Program Title	Amount	Method/Basis of Valuation
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs	$ 52,602	Per authorized award for personnel costs and travel.
93.268	Immunization Grants	12,775,047	Per authorized award for personnel, vaccine costs, and travel.
93.283	Centers for Disease Control and Prevention – Investigations and Technical Assistance	49,343	Per authorized award.
93.940	HIV Prevention Activities – Health Department Based	11,599	Per authorized award.
93.977	Preventive Health Services – Sexually Transmitted Diseases Control Grants	333,506	Per authorized award.
	Total Noncash Expenditures	$ 13,222,097	

Note 4 - Research and Development Expenditures

OMB Circular A-133 Section 105 states, "Research and development (R&D) means all research activities, both basic and applied, and all development activities that are performed by a non-Federal entity."

CFDA #	Program Title	Expenditures
93.230	Consolidated Knowledge Development and Application (KD&A) Program	$ 308,131
93.238	Cooperative Agreements for State Treatment Outcomes and Performance Pilot Studies Enhancement	210,629
	Total R&D Expenditures	$ 518,760

Note 5 - Zero Expenditure Programs

These programs had no expenditures related to the respective state organization during FY 04. The zero expenditure programs included programs with no activity during the year, such as old programs not officially closed out or new programs issued late in the fiscal year. They also included programs with activity other than expenditures. For CFDA numbers with multiple state organizations listed, the schedule is presented in descending expenditure amount order.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-1: The Cabinet for Health Services Should Provide Better Safeguards For Funds Placed In Its Care

State Agency: Cabinet for Health Services
Federal Program: CFDA 93.778 – Medicaid Assistance Program
Federal Agency: U.S. Department of Health and Human Services
Pass-Through Agency: Not Applicable
Compliance Area: Allowable Costs
Amount of Questioned Cost: None

In previous years the APA has issued comments in the area of SMI for failing to reconcile agency reports against UNISYS reports to determine that valid claims were properly processed and paid. However, the agency has made an effort in the past year to resolve this issue and provide corrective action to include this control as part of administering the program.

However, during fieldwork of the fiscal year 2004 audit, and as part of the ongoing agency effort to reconcile system information, the APA became aware of a situation that caused the Department for Medicaid Services (DMS) to expend an approximate $5,000,000 additional dollars for one month of premiums for Supplementary Medical Insurance (SMI). As a result of revised programming efforts, a large number of eligible participants were removed from the Medicaid roll, as well as, a number of ineligible participants being added to the Medicaid roll. DMS has made efforts to recoup any ineligible payments.

SMI payments made during fiscal year 2005 included:

July -	$ 9,016,941
August -	$ 8,749,306
September -	$ 8,602,681
October -	$14,129,211
November -	$ 9,035,492
December -	$ 7,351,565

A simple trend analysis of Medicaid payments made during fiscal year 2005 would have indicated a large spike in payments from September to October. Although performing such analysis may not be a necessary control feature, having done such an analysis may have prevented an error of this magnitude from occurring.

The APA is continuing review of this matter and will be coordinating audit work with federal agencies.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-1: The Cabinet for Health Services Should Provide Better Safeguards For Funds Placed In Its Care (Continued)

When the state overpays any bill by $5 million questions must be asked to ensure the over sight agency is properly safe guarding the assets of the Commonwealth. During times of short falls and budget crisis even more emphasis must be placed on safeguarding and protecting every dollar. This problem is that the state spent money it did not need to.

The State should ensure through its financial internal controls that when invoice/premium payments jump by a large and/or unusual amount that those in higher positions in the cabinet are notified. Corrective action should be taken or at least attempted before issuing payments. We acknowledge this would be difficult for the DMS in this area since a refusal to pay would have cost thousands of citizens their health insurance, while the problem was resolved. However by attempting this they could have at least demonstrated that internal controls were operating as designed and effective.

Recommendation

We recommend that DMS as well as CHFS review its payment procedures so that large jumps in contract/premium amounts are not paid "just because that was the amount they sent me". DMS and CHFS should ensure that every effort is made to not only secure the health and medical needs of the citizens of the Commonwealth but to secure their financial responsibility to the citizens.

Management's Response and Corrective Action Plan

Background:

At issue is the Kentucky Department for Medicaid Services' (DMS) submission to the Centers for Medicare and Medicaid Services (CMS) of the DMS Buy-In Input file containing August 2004 accretion and deletion data. This file, which was submitted to CMS at the end of August 2004, was found to have contained erroneous data.

The data was contained on the Social Security Administration (SSA) Beneficiary Data Exchange file (BENDEX), which is received by DMS on a semi-monthly basis. A number of legitimate entitlements had erroneously been deleted (around 12,000). This accretion resulted in the expenditure of approximately $5 million total funds for Buy-In premium payments.

Additionally, approximately 4,800 new individuals were accreted as a result of a one-time issue that occurred during the processing of the Department's August recipient file.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-1: The Division Of Medicaid Services Should Provide Better Safeguards For Funds Placed In Its Care (Continued)

Management's Response and Corrective Action Plan (Continued)

Around early September DMS learned of issues related to the August file. As a result, DMS worked with CMS to resolve the issue and received permission from CMS to recreate the file. In the interest of time, DMS was advised by CMS to first take action to restore the deleted eligibles. Additionally, DMS was advised by CMS to then delete the accreted recipients after restoring the deleted recipients to full benefit status. Consequently, the new Input file due at the end of September 2004 had to be sent to CMS prior to DMS completion of the deletions in order to meet CMS timeframe for processing the file.

After processing the Input file, CMS submitted to DMS the Buy-In Billing file in early September, which included accretion files created by CMS. As a result of CMS processing the August Input file, Buy-In payments became due and were paid in the month of October totaling $14,129,211.

DMS had anticipated a high level of activity on its August Buy-In file due to changes DMS made to its internal Buy-In file. In addition, CMS had made changes to Buy-In file layout and required states to follow new CMS procedures for the first time in August.

As soon as DMS learned of the issues with the file, DMS personnel immediately began working with CMS to take corrective action. DMS identified the discrepancy on the file during the second week of September 2004 and immediately contacted CMS to request permission to submit a modified Buy-In file to reverse the transactions, thereby averting an overpayment of funds. CMS policy does not provide for reversal of the transactions on the basis of the above-mentioned federal regulation, which states that once a file has been processed by CMS it will not be considered erroneous. 42 CFR 407.47(e).

In September, DMS also requested reconsideration by CMS based on the payment amount in question. CMS did not reconsider and informed DMS that other states had made the same error. The example cited concerned New Jersey, which refused to make the premium payments as billed based on the erroneous data. As a result, the amount in question was deducted from New Jersey's regular Medicaid federal funding. In addition, DMS recouped as many of the premium payments as allowed by federal law, which states that only three months of premium payment may be recouped.

Internal controls have been added to insure that any future changes to the Buy-In subsystem are approved at a director level. Currently, DMS continues its efforts to further refine the Buy-In process. DMS is also utilizing current consultants to evaluate further corrective action.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-1: The Division Of Medicaid Services Should Provide Better Safeguards For Funds Placed In Its Care (Continued)

Management's Response and Corrective Action Plan (Continued)

Agreement:

The Department for Medicaid Services agrees with the Auditor of Public Account's (APA) recommendation that DMS should "review its payment procedures" and has taken active steps to insure accuracy in the Buy-in payment process.

Due to the specification of 42 CFR 407.47(e), which states that "…If the state erroneously reports to SSA that an individual is a member of its coverage group, the rules of paragraphs (a) through (d) of this section apply, and coverage begins as though the individual were in fact a member of the group", corrective action has been implemented which ensures that all Buy-In files are reviewed and analyzed by DMS and Medicaid's fiscal agent (Unisys) staff prior to submission to CMS to identify and correct any inaccuracies.

Internal controls have been put in place through coding changes made to the Medicaid Management Information System (MMIS) to prevent a reoccurrence of this issue.

Currently, DMS personnel are manually reviewing the BENDEX data utilizing other data sources in order to prevent a reoccurrence of the situation.

In addition, Medicaid is utilizing consultants to provide advice to the Department regarding implementation of additional internal controls including utilizing multiple files, or data sources, to verify the information DMS sends to CMS.

As a consequence of the August Buy-In events, the Kentucky Department of Justice and the Kentucky Office of the Inspector General are investigating DMS for the payments made to the recipients accreted in the August file. This investigation is ongoing and any findings will be utilized to implement further improvements to the Buy-In subsystem.

The Department for Medicaid Services appreciates the connotation of the APA's statement regarding the difficulty DMS would have experienced if it had simply refused to pay the indicated amount of Buy-In. That option would have placed thousands of Kentucky citizens in danger of losing their health insurance coverage.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-2: The Department For Public Health Should Improve Efforts In Monitoring Subrecipient Activity

State Agency: Cabinet for Health Services
Federal Program: CFDA 93.283 – Centers for Disease Control and Prevention Investigations and Technical Assistance
Federal Agency: U.S. Department of Health and Human Services
Pass-Through Agency: Not Applicable
Compliance Area: Subrecipient Monitoring
Amount of Questioned Cost: None

The Department for Public Health (DPH) is responsible for monitoring subrecipient's use of federal awards. DPH performs monitoring through periodic site visits. The site visits assist in providing reasonable assurance that subrecipients administer federal assistance programs in compliance with laws, regulations, and the provisions of contracts or grant agreements and ensure that performance goals are achieved. DPH also has the responsibility to take prompt corrective action on any monitored audit findings within a reasonable time frame.

For fiscal year 2004, in addition to requiring site visits for those receiving federal awards, the department was required to have audits performed for 11 subrecipients who received $5,490,369 of $10,061,885 sent to subrecipients.

For testing purposes, we chose six (6) facilities that reported findings as a result of a site visit. For these site visits that resulted in any findings, we requested the corrective action plans for those facilities. Corrective actions plans for those facilities had either not been developed and/or implemented, until the request by the APA was made. Thus, DPH is not following up with their responsibility to monitor subrecipients and their plans for corrective action. They acknowledged this shortcoming in an email to the APA in which DPH states they are beginning to correct this problem

The Department for Public Health cannot be assured that the expended federal awards were for their intended purpose and complied with the requirements of OMB Circular A-133 without having proper monitoring procedures in place. We were unable to determine if the Department for Public Health evaluated the impact of subrecipient activities on the federal program and took timely and appropriate corrective action on any findings.

The Department for Public Health has the following responsibilities under OMB Circular A-133, Subpart D:

1) Ensure that subrecipients take prompt corrective action on any monitored audit findings; and,

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 04-CHS-2: The Department For Public Health Should Improve Efforts In Monitoring Subrecipient Activity (Continued)

2) Evaluate the impact of subrecipient activities on the pass-through entity's ability to comply with applicable Federal regulations.

Recommendation

We recommend that the Department of Public Health ensure that A) appropriate corrective actions are taken on any subrecipient monitoring findings, and B) the auditors are able to review program compliance in the future.

Management's Response and Corrective Action Plan

This comment specifically concerns the financial management portion of the local agency review, which is conducted by the Division of Administration and Financial Management.

Corrective action has been taken by the Division. Effective July 1, 2004, the Division will monitor each local agency this state fiscal year. The Division is currently on track to complete all of the reviews by June 20, 2005. A tracking process is in place to ensure the site reviews are on schedule. Once this state fiscal year is completed, the Division will return to reviewing each local agency once every two years.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-3: The Department For Public Health Should Improve Efforts In Monitoring Subrecipient Activity

State Agency: Cabinet for Health Services
Federal Program: CFDA 10.557 – Special Supplemental Nutrition Program for Women, Infants, and Children
Federal Agency: U.S. Department of Agriculture
Pass-Through Agency: Not Applicable
Compliance Area: Subrecipient Monitoring
Amount of Questioned Cost: None

The Department for Public Health (DPH) is responsible for monitoring subrecipient's use of federal awards. DPH performs monitoring through periodic site visits. The site visits assist in providing reasonable assurance that subrecipients administer federal assistance programs in compliance with laws, regulations, and the provisions of contracts or grant agreements and ensure that performance goals are achieved. DPH also has the responsibility to take prompt corrective action on any monitored audit findings within a reasonable time frame.

For certain site visits that resulted in any findings, we requested the corrective action plans for those facilities. Corrective actions plans for those facilities had either not been developed and/or implemented, until the request by the APA was made. Thus, DPH is not following up with their responsibility to monitor subrecipients and their plans for corrective action. They acknowledged this shortcoming in an email to the APA in which DPH states they are beginning to correct this problem.

The Department for Public Health cannot be assured that the expended federal awards were for their intended purpose and complied with the requirements of OMB Circular A-133 without having proper monitoring procedures in place. We were unable to determine if the Department for Public Health evaluated the impact of subrecipient activities on the federal program and took timely and appropriate corrective action on any findings.

The Department for Public Health has the following responsibilities under OMB Circular A-133, Subpart D:

- Ensure that subrecipients take prompt corrective action on any monitored audit findings; and,
- Evaluate the impact of subrecipient activities on the pass-through entity's ability to comply with applicable Federal regulations.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-3: The Department For Public Health Should Improve Efforts In Monitoring Subrecipient Activity (Continued)

Recommendation

We recommend that the Department of Public Health ensure that A) appropriate corrective actions are taken on any subrecipient monitoring findings, and B) the auditors are able to review program compliance in the future.

Management's Response and Corrective Action Plan

It is agreed that the WIC Program federal regulations 7 CFR Part 246.19 (b)(3) state that - The State Agency shall conduct monitoring reviews of each local agency once every two years. This comment specifically concerns the financial management portion of the local agency review, which is conducted by the Division of Administration and Financial Management.

The Division has taken corrective action. Effective July 1 2004, the Division will monitor each local agency this state fiscal year. The Division is currently on track to complete all of the reviews by June 30, 2005. A tracking process is in place to ensure the site reviews are on schedule. Once this state fiscal year is completed, the Division will return to reviewing each local agency once every two years.

FINDING 04-CHS-4: The Division Of Program Integrity Should Track Interest Due On Outstanding Drug Rebate Balances

State Agency: Cabinet for Health Services
Federal Program: CFDA 93.778 – Medical Assistance Program
Federal Agency: U.S. Department of Health and Human Services
Pass-Through Agency: Not Applicable
Compliance Area: Allowable Costs
Amount of Questioned Cost: None

The Division of Program Integrity does not track interest due on outstanding balances for the Drug Rebate Program. The APA inquired if anyone calculated interest on the outstanding balances and was informed Unisys only tracked interest received from Drug Manufacturers. DMS has the responsibility to track the amount of interest due from each manufacturer.

Although we continue to note a failure to track interest due on outstanding drug rebate balances, we were informed that during FY 05 First Health Services Corporation was contracted to oversee the tracking of interest and help resolve the backlog of disputes. This will hopefully, eliminate future problems with tracking interest due, and improve the ability to resolve disputed claims.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-4: The Division Of Program Integrity Should Track Interest Due On Outstanding Drug Rebate Balances (Continued)

The Medicaid Drug Rebate Program, created by the Omnibus Budget Reconciliation Act (OBRA) of 1990 states:

> The balance due, if any, plus a reasonable rate of interest as set forth in section 1903(d)(5) of the Act, will be paid or credited by the Manufacturer or the State by the due date of the next quarterly payment in II(b) after resolution of the dispute.

Since DMS is not tracking interest, the state potentially could be losing several thousand dollars to offset the federal match. Drug manufacturers are responsible for calculating and paying the proper interest rates. However, this does not relieve DMS of the responsibility of control over this area and determining which manufacturers should be paying interest and how much interest they should be receiving.

Government entities should maintain control over accounts receivables as stewards of public funds. Allowing companies to calculate and pay interest with no checks or oversight allows for discrepancies and is a lack of control.

Recommendation

We recommend the Division of Program Integrity calculate and track interest due on outstanding balances so comparisons can be made to manufacturers payments and any discrepancies corrected.

Management's Response and Corrective Action Plan

The drug rebate program is now coordinated through Medicaid's Financial Management Branch. In order to better manage the responsibilities assigned to the branch, including the drug rebate program, the branch's duties have been examined and revised.

In addition to maximizing internal resources, the Department contracted with a pharmacy benefits administrator (First Health Services Corporation) to administer the pharmacy program, effective December 4, 2004. FHSC's system provides for the application, accrual and collection of interest due on drug rebates. Interest is applied to unpaid rebate amounts and to late rebate payments. Due to the emphasis placed on this program and the corresponding contract, DMS has received approval to hire two additional personnel for contract oversight.

FHSC has begun implementing procedures to track and accrue interest. Using its standard monitoring protocols, DMS is confident that federal guidelines regarding drug rebate interest will be followed.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-5: The Division Of Program Integrity Should Improve Efforts In Resolving The Backlog Of Disputes Relating To Outstanding Accounts Receivable Balances In The Drug Rebate Program

State Agency: Cabinet for Health Services
Federal Program: CFDA 93.778 – Medical Assistance Program
Federal Agency: U.S. Department of Health and Human Services
Pass-Through Agency: Not Applicable
Compliance Area: Allowable Costs
Amount of Questioned Cost: None

The Division of Program Integrity, historically, has not been actively seeking payment on accounts receivable after a second notice has been sent. The division sends a notice to delinquent drug manufacturers after 38 days. Another notice is sent after 60 days to request payment or reason for amount disputed. After the second notice is sent there are no other formal attempts made at settlement.

During the FY 2003 audit, DMS stated that they were working to resolve the backlog of complaints for drug rebate and that one of two things would occur, either 1) a Pharmacy Benefits manger would be added to address the backlog of accounts receivable; or 2) Unisys functions would be added to monitor and track interest.

During FY 2004, neither of these occurred, but the auditor learned that during FY 2005, DMS has contracted with First Health Services Corporation to begin overseeing and assisting DMS with the backlog of disputes and handling the present ones, plus tracking interest. Also noted was that DMS is attempting to hire two positions to help work on the backlog of disputes, and oversee the contract.

Going forward, the APA will continue to monitor this area, as we aren't able to yet determine if this has corrected the problem.

As of June 30, 2004, accounts receivable balance for the Drug Rebate program was $60,470,326.26 since June 30, 1991. For FY 04 the amount outstanding is $27,987,994.29. Medicaid is potentially losing millions of dollars that could help offset budget deficits in the coming and present fiscal year.

The Medicaid Drug Rebate Program, created by the Omnibus Budget Reconciliation Act (OBRA) of 1990 states the following:

> Except as provided under V(b), to make such rebate payments for each calendar quarter within 30 days after receiving from the State the Medicaid Utilization Information defined in this agreement. Although a specific amount of information has been defined in I(n) of this agreement, the Manufacturer is responsible for timely payment of the rebate within 30 days of receiving, at a minimum, information on the number of units paid,

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-5: The Division Of Program Integrity Should Improve Efforts In Resolving The Backlog Of Disputes Relating To Outstanding Accounts Receivable Balances In The Drug Rebate Program (Continued)

> by NDC number. In the event that in any quarter a discrepancy in Medicaid Utilization Information is discovered by the Manufacturer, which the Manufacturer and the State in good faith are unable to resolve, the Manufacturer will provide written notice of the discrepancy, by NDC number, to the State Medicaid Agency prior to the due date in II(b). If the Manufacturer in good faith believes the State Medicaid Agency's Medicaid Utilization Information is erroneous, the Manufacturer shall pay the State Medicaid Agency that portion of the rebate amount claimed which is not disputed within the required due date in II (b).

In addition, proper accounting procedures for accounts receivables require balances be monitored and immediate action taken for outstanding balances.

Recommendation

We recommend that the accounts receivable balance, continue to be monitored, and collection procedures continue, while the Auditor's Office will continue to monitor this area.

Management's Response and Corrective Action Plan

The Department for Medicaid Services (DMS) wishes to clarify the oversight of the drug rebate program. The program is now coordinated through Medicaid's Financial Management Branch. In order to better manage the responsibilities assigned to the branch, including the drug rebate program, the branch's needs and duties have been examined and revised.

In an attempt to maximize internal resources, the Department contracted with a pharmacy benefits administrator First Health Services Corporation (FHSC). FHSC began administering the pharmacy program, effective December 4, 2004. Resolving and collecting outstanding drug rebate accounts receivables is included in FHSC's responsibilities. Due to the emphasis placed on this program; and the corresponding contract, DMS has received approval to hire two additional personnel for contract oversight.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-5: The Division Of Program Integrity Should Improve Efforts In Resolving The Backlog Of Disputes Relating To Outstanding Accounts Receivable Balances In The Drug Rebate Program (Continued)

Management's Response and Corrective Action Plan (Continued)

FHSC takes a proactive approach in drug rebate invoicing. Data is reviewed prior to invoicing in order to reduce the incidence of avoid erroneous billing. If invoiced amounts are disputed, specific steps are outlined within the DMS and FHSC contract are followed to resolve rebate disputes. Dispute resolution procedures are based upon the official CMS "Best Practices for Dispute Resolution Under the Medicaid Drug Rebate Program". The guidelines FHSC will follow are listed below.

- *Acknowledge receipt of dispute with labeler within 2 business days;*
- *Present a preliminary dispute response to the labeler, specifically addressing the dispute reason indicated by the labeler, within 15 days of receipt of the dispute;*
- *Contact the labeler to discuss units disputed by NDC and the reason(s) for the dispute; within 90 days after the labelers dispute;*
- *Take steps to resolve questionable data within 150 days after receipt of the labelers dispute;*
- *If FHSC finds that attempts to resolve a dispute with a labeler remains unsuccessful after 240 days, FHSC should forward the complaint and detailed pattern of non-responsiveness to the State for discussion.*
- *FHSC contacts labelers by phone and e-mail in an attempt to resolve disputes. In addition to the phone and e-mail contacts, FHSC representatives attend dispute resolution conferences in order to meet directly with the labelers and to resolve issues.*

DMS is encouraged to settle disputes resulting from inaccurate invoices. Disputes arising prior to the FHSC takeover will be resolved with FHSC assistance. Our in-house staff will closely monitor the contract and the actions of FHSC in order to ensure appropriate action is taken and all regulations are followed.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-6: The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized

As noted in the prior audit, the Cabinet for Health Services (CHS) did not restrict critical information divulged by its network machines. During examination of the CHS local area networks (LANs) security for fiscal year 2004, we discovered several instances in which machines within the LANs provided information that could potentially assist an intruder in developing an approach to attack the system.

Using standard scanning tools we examined the machine names and other remarks located within seven CHS domains. The naming convention of machines was not sufficiently ambiguous to disguise the function of machines in two domains. Further, descriptive comments might catch an intruder's interest. Out of 2,516 machines examined, 345, or 13.7% had comments that could be beneficial to unauthorized users. Both of these findings had been reported to the agency during the prior year audit.

We also ran other vulnerability assessment tools during the current fiscal year on 72 machines within the CHS domains to determine if information would still be returned for Local Security Authority (LSA), Password Policies, Valid User, Group, or Share Lists. The table below depicts the number of machines that would provide this information.

Type of Information	Number of machines providing information	Percentage of 72 machines providing information
LSA	44	61.1%
Password Policies	29	40.2%
Valid User List	29	40.2%
Valid Group List	29	40.2%
Valid Share List	28	38.8%

An agency's domain information that is accessible to the world at large through inquiry tools should be kept at a minimum. Agencies should ensure that information such as location, accounts associated with the machine, type of data residing on the machine, and the machine's role are not divulged or is stated in the most minimal of terms. To accomplish this, an agency can set devices to not respond to certain types of inquiries, use naming conventions that obscure the purpose of machines, and omit comments on machine activity.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-6: The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized (Continued)

Recommendation

We recommend that CHS continue their efforts to restrict the level of information provided by their LAN machines to anonymous users. First, the naming convention of machines and descriptive comments should be altered to make them more ambiguous where it is possible before the Active Directory structure is established. Second, limitations should be placed on the type of response the machines provide based on certain inquiries.

Management's Response and Corrective Action Plan

We are not disputing that this leakage of information is a vulnerability, but we do believe that this issue does not warrant the investment of resources (this would require each machine to be manually reconfigured) needed to bring this into immediate compliance. Efforts will be ongoing until such time as we achieve complete compliance. The naming convention is being altered as each machine is migrated into the AD environment.

Migration into the AD domain is a slow and resource intensive process and has been further impacted by the recent cabinet merger. The issue of unnecessary comments can be corrected with minimal resources and will be immediately addressed.

FINDING 04-CHS-7: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose

During the security vulnerability assessment testing for machines controlled by the Cabinet for Health Services (CHS) for fiscal year 2004, we found several CHS machines with ports open that may not have a specific business-related purpose. The findings are grouped by port number and application.

Port 21 File Transfer Protocol (FTP): Two machines were noted with this port open allowing administrator and anonymous access to a session without requiring a password.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-7: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose (Continued)

Port 80 Hypertext Transfer Protocol (HTTP): Three machines displayed the message that the site was under construction and the site was not found for one machine. These should be reviewed for the necessity of this open port. These four machines had been noted with this issue in the prior audit. Second, configuration information for printers or print machines was provided by three websites, which were also noted in the prior year audit. This latter situation allows too much access to an unauthorized or anonymous user and should be further protected.

Port 443 Hypertext Transfer Protocol over Secure Socket Layer (HTTPS/SSL): Nine machines were found with port 443 open but would not display a website. Six of these machines were noted with this issue in the prior audit. When no default page or restricted logon is required, normally this means that no application/web service is running at the port. The necessity of these ports should be reviewed. Also, two additional machines required login access although multiple guess attempts were allowed. These login attempts should be restricted.

Ports 5225 - 5226 Unassigned: One machine was found with both ports 5225 and 5226 open. This port has not been assigned per IANA and further research revealed no information or vulnerabilities. This open port should be reviewed for necessity.

Port 5397 Unassigned: One machine was found with this port open. Although vulnerabilities associated with this port were not determined, it should be reviewed for business necessity.

Port 5631 PCAnywhere Data: Three machines were found with port 5631 open. This port listens on other ports to find other PCAnywhere servers on the local segment. Vulnerabilities may exist in the form of denial of service attacks. Two of these machines have been reported in prior audits. Previous responses from CHS have not indicated these ports – services are specifically necessary. They should be reviewed and, if necessary, ensure they are properly protected.

Port 5679 Direct Cable Connect Manager (DCCM): One machine was found with this port open. Although vulnerabilities associated with this port were not determined, it should be reviewed for business necessity.

Ports 5800 and 5900 Virtual Network Computer (VNC): Two machines had both of these ports open. VNC allows the possibility to view and interact with one computer from any other computer or mobile device. This should be reviewed for business-related necessity and to ensure strong protection measures have been taken.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-7: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose (Continued)

Port 5812 Unassigned: One machine was found with this unassigned port open. CHS prior assessment responses regarding this machine indicated it requires various open ports but this port was not specifically mentioned. This port should be reviewed for business necessity.

Ports 5881 and 5981 Unassigned: Two machines were found with both of these unassigned ports open. Research revealed backdoor Trojan horse vulnerabilities with port 5881. These ports should be reviewed for business necessity and to ensure strong protection measures have been taken if the service is needed.

To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open. Further, the application residing at these ports should be secured to the extent possible.

Recommendation

We recommend that CHFS (formerly CHS) perform a review of the services running on the noted open ports. If there is not a specific business-related purpose requiring the service, then the service should be closed. If the service is necessary, then CHFS should ensure adequate logical security controls have been implemented to prevent unauthorized access. Further, we recommend that CHFS periodically review of open ports on all machines owned by the agency to ensure necessity of underlying services.

Management's Response and Corrective Action Plan

Each open port listed will be reviewed for necessity and if deemed necessary evaluated to see if all available means of maximizing security have been implemented. Many of the ports listed in this initial report are required to maintain the functionality of the CHFS network but can be made more secure by limiting access at the CHFS firewall. The CHFS security team will address each of these on an individual basis.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-8: The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers

As was noted in the prior audit reports, password policies established on certain critical Cabinet for Health Services (CHS) machines did not adhere to the Commonwealth Office of Technology (COT) or CHS password policies. During the FY 2004 audit, testing was performed to determine the accessibility of the password policies of machines within the seven CHS domains using vulnerability assessment tools. Password policies obtained were reviewed for compliance to established policy standards. Of 72 machines tested, we were able to obtain the password policies for 29, or 40 percent, of these machines. See findings below.

Security Measure	COT Security Policy	Number of machines noncompliant (Out of 29 machines)
Minimum Length	8 characters	7 characters - 5 0 characters – 17 *Five noted in prior audit report*
Minimum Age	1 day	0 days – 24 *Ten noted in prior audit report*
Maximum age	31 days	30 days – 2 42 days – 17 45 days – 5 *Twelve noted in prior audit report*
Lockout Threshold	3 attempts	0 attempts – 17 *Five noted in prior year report*

Passwords are a significant feature to guard against unauthorized system access. The purpose of a password policy is to establish a standard to create strong passwords, to protect those passwords, and to ensure passwords are changed within a specified time period. To assist in the security of a network, it is necessary for a strong policy to be developed and consistently implemented on all machines throughout the network.

We have noted from prior audit responses to this issue that CHS has adopted a stringent network password policy with few exceptions. These exceptions involve agreements between CHS and other agencies that were expected to be implemented early 2004. Also, additional corrections are expected to be implemented once the anticipated Active Directory structure is established. This is not expected to occur until all necessary agency updates to equipment are in place, which have been delayed.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-8: The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers (Continued)

Recommendation

We recommend that CHS periodically review all machines within its agency-owned domains to ensure that the password policy established on the machines complies with the guidelines specified by the agency and COT. Further, procedures should be established to periodically review these settings for all CHS machines and ensure all accounts comply with the established password policy. We further recommend CHS consider alternative security measures for remaining concerns if the implementation of the new directory structure continues to be delayed.

Management's Response and Corrective Action Plan

There are two types of password policies in our environment one being the domain password policy and the other being the local password policy which resides on each workstation and server on our network. The domain policy is the more critical of the two and all CHFS user accounts use domain accounts to access resources on our network. Of the nine domains, two domains (LHD & the Commission) were out of compliance. One domain was fixed and the other will be brought into compliance within the next month. The effort will be done incrementally. We standardized the password policy on all CHFS domain PDCs to reflect the COT standard." The local policies will be brought into compliance in the AD domain through the use of Group Policy Objects (GPO). Our current environment would require manual reconfiguration of each machine and would be extremely resource intensive. The use of GPO's in the AD domain will allow us to correct this on all machines by simply applying this policy at the domain level. Any servers listed in the detailed report that are out of compliance will be immediately addressed.

Auditor's Reply

Further investigation revealed nine of our twenty-six machines noted above were either Primary Domain Controllers (PDCs) or Backup Domain Controllers (BDCs). At the time of fieldwork none of these machines was compliant with COT password policy standards. Following response from the agency we acknowledge that the only PDCs and BDCs that remain noncompliant are within the domain that the agency intends to bring to standards incrementally as noted in their response. It is reasonable to assume the remaining seventeen local machine's password polices should be compliant once they implement the GPO.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 04-CHS-9: The Cabinet For Health Services Should Strengthen The Security Of System Accounts

Security vulnerability testing for FY 2004 on machines controlled by the Cabinet for Health Services (CHS) revealed several instances of lax security over default system accounts resulting in the potential of servers being vulnerable to intrusion. We tested 62 machines using vulnerability assessment tools and were able to obtain NetBios information on 27 of those machines. Examination of the information obtained revealed 14 machines with the default administrator account that had not been renamed adequately, three of which had been noted in the prior audit report with this same issue. Further, we noted 23 machines for which the default guest account had not been disabled. Five of these machines had been noted in the prior audit report with this same issue.

Default system accounts can allow access to the system and must be adequately secured. Guest account must be disabled. Further, the default passwords on the accounts must be changed and comply with the CHS password policy.

Recommendation

We recommend that CHS review all servers to ensure that the system administrator accounts have been renamed from default naming conventions to more ambiguous names, and that default guest accounts have been disabled. We further recommend these reviews be performed on a periodic basis throughout the year. CHS policies dictate that default administrator accounts must be renamed and the default

Management's Response and Corrective Action Plan

All CHFS servers will be reviewed to ensure that the Guest account has been disabled (where applicable) and the Administrator account renamed. Under our current configuration this cannot be done automatically and will require periodic review by CHFS security staff. Once fully migrated into AD this can be automated through GPO's to ensure that 100% compliance is achieved and maintained.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2004

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Reportable Conditions					
(1) Audit findings that have been fully corrected:					
FY 03	03-CHS-1	The Vital Statistics Branch Should Improve Controls Over Assets And Separate Work Tasks	N/A	0	Resolved during FY 04.
FY 03	03-CHS-2	The Vital Statistics Branch Should Take Steps To Reduce The Identity Theft Risks	N/A	0	Resolved during FY 04.
FY 02	02-CHS-2	The Vital Statistics Branch Should Improve Controls Over Assets And Separate Work Tasks	N/A	0	Resolved during FY 04.
FY 02	02-CHS-3	The Vital Statistics Branch Should Take Steps To Reduce The Identity Theft Risks	NA	0	Resolved during FY 04.
FY 01	01-CHS-4	The Vital Statistics Branch Should Improve Security Over Assets And Segregate Job Duties	N/A	0	Resolved during FY 04.
FY 01	01-CHS-6	The Vital Statistics Branch Should Take Steps To Prevent Identity Theft	NA	0	Resolved during FY 04.
Audit findings not corrected or partially corrected:					
No findings for this section.					
(3) Corrective action taken is significantly different from corrective action previously reported:					
No findings for this section.					
(4) Audit finding is no longer valid and does not warrant further action:					
No findings for this section.					

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2004

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments

Material Weaknesses/Noncompliances

(1) Audit findings that have been fully corrected:

No findings for this section.

(2) Audit findings not corrected or partially corrected:

No findings for this section

(3) Corrective action taken is significantly different from corrective action previously reported:

No findings for this section

(4) Audit finding is no longer valid and does not warrant further action:

No findings for this section.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2004

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters					
(1) Audit findings that have been fully corrected:					
FY 03	03-CHS-3	The Cabinet For Health Services Should Remove The Simple Network Management Protocol Service Or Change The Default Community String	N/A	0	Resolved during FY 04.
FY 03	03-CHS-9	The A-133 Audits Of Subrecipients Need To Have A Timely Desk Review	93.044 and 93.045	0	Resolved during FY 04.
FY 03	03-CHS-10	Aging Should Conduct On-Site Monitoring Visits To Each Area Development District During A Fiscal Year	93.044 and 93.045	0	Resolved during FY 04.
FY 03	03-CHS-10	Aging Should Conduct On-Site Monitoring Visits To Each Area Development District During A Fiscal Year	93.044 and 93.045	0	Resolved during FY 04.
FY 02	02-CHS-7	The Cabinet For Health Services Should Remove The Simple Network Management Protocol Service Or Change The Default Community String	N/A	0	Resolved during FY 04.
FY 02	02-CHS-16	The Office Of Aging Does Not Document The Performance Of Desk Reviews	93.044 and 93.045	0	Resolved during FY 04.
FY 02	02-CHS-17	The Office Of Aging Did Not Make Monitoring Visits To All Area Agencies	93.044 and 93.045	0	Resolved during FY04.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2004

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters (Continued)					
(2) Audit findings not corrected or partially corrected:					
FY 03	03-CHS-4	The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized	N/A	0	Exceptions were still noted for FY 04 See 04-CHS-6
FY 03	03-CHS-5	The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose	N/A	0	Exceptions were still noted for FY 04 See 04-CHS-7
FY 03	03-CHS-6	The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers	N/A	0	Exceptions were still noted for FY 04 See 04-CHS-8
FY 03	03-CHS-7	The Division Of Program Integrity Still Has A Big Outstanding Balance Of Accounts Receivable For the Drug Rebate Program	93.778	0	No apparent attempts have been made by the agency to resolve this. An outside contractor has been hired to help with this matter in FY2005 See 04-CHS-5
FY 03	03-CHS-8	The Division Of Program Integrity Still Does Not Track Interest Due On Outstanding Drug Rebate Accounts	93.778	0	No apparent attempts have been made by the agency to resolve this. An outside contractor has been hired to help with this matter in FY2005 See 04-CHS-4
FY 03	03-CHS-11	The Department For Public Health Needs To Ensure Corrective Actions Are Taken On Subrecipient Monitoring.	93.283	0	Upgraded to reportable this year. See 04-CHS-2
FY 02	02-CHS-4	The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized	N/A	0	Exceptions were still noted for FY 04. See 04-CHS-6
FY 02	02-CHS-5	The Cabinet For Health Services Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose	N/A	0	Exceptions were still noted for FY 04. See 04-CHS-7

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2004

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters (Continued)					
(2) Audit findings not corrected or partially corrected (Continued):					
FY 02	02-CHS-6	The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers	N/A	0	Exceptions were still noted for FY 04 See 04-CHS-8
(3) Corrective action taken is significantly different from corrective action previously reported:					
No findings for this section.					
(4) Audit finding is no longer valid and does not warrant further action:					
No findings for this section.					